Assignment : Public key cryptography - PracticalScenario

- ## RSA Encryption :

Under RSA encryption, messages are encrypted with a code called a public key, which can be shared openly. Due to some distinct mathematical properties of the RSA algorithm, once a message has been encrypted with the public key, it can only be decrypted by another key, known as the private key. Each RSA user has a key pair consisting of their public and private keys. As the name suggests, the private key must be kept secret.

Public key encryption schemes differ from symmetric-key encryption, where both the encryption and decryption process use the same private key. These differences make public key encryption like RSA useful for communicating in situations where there has been no opportunity to safely distribute keys beforehand.

- ## Why we need this kind of encryption ?

Traditional encryption consists of only one key to encrypt and decrypt the data. That means if you want to send something sensitive data then you have to select a key and share it with other person securely and then then you can send and receive data securely and decrypt it accurately. But what if you don't have secure line to send the key or you didn't give the key beforehand then this tradition encryption will not work.

RSA encryption solve this problem by having two key pair (public , private) where public will encrypt the message and private will decrypt the message. This public key will be shared openly because this key doesn't decrypt the message , in other words , it is useless to decode the message.

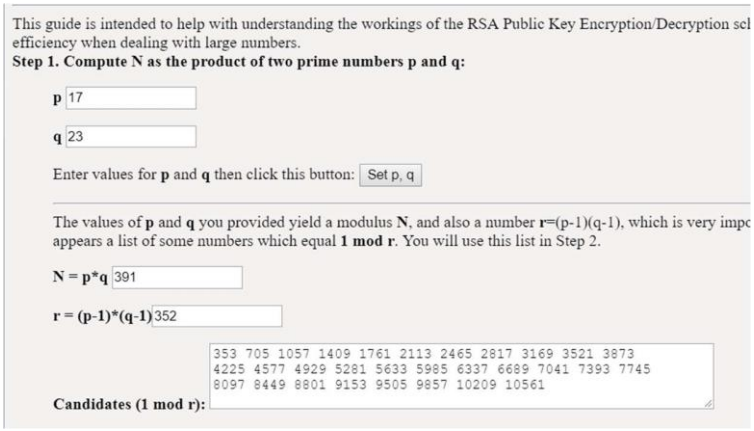
- ## How the algorithm works?

 Step 1:

Select Two prime numbers (they should be far apart because nearer values are easy to crack) In current example we selected p = 17 , q = 23 ,

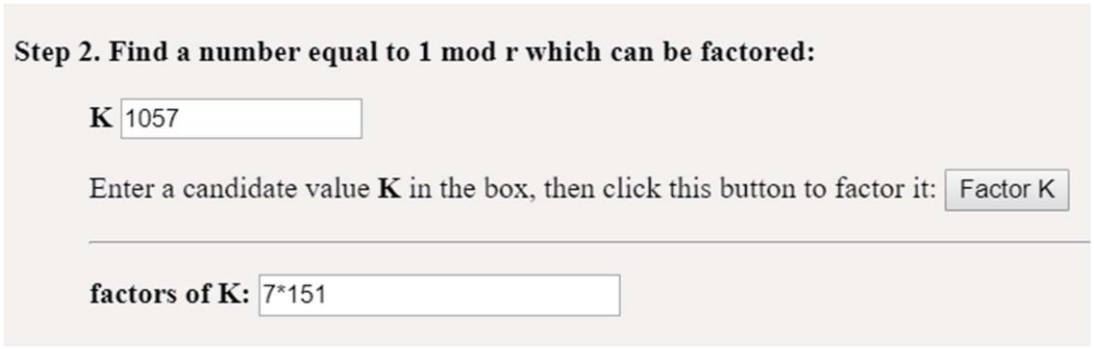
N = 17*23 = 391 , r = (17-1)*(23-1) =352

Note : The prime numbers in RSA need to be very large, and also relatively far apart. Numbers that are small or closer together are much easier to crack.



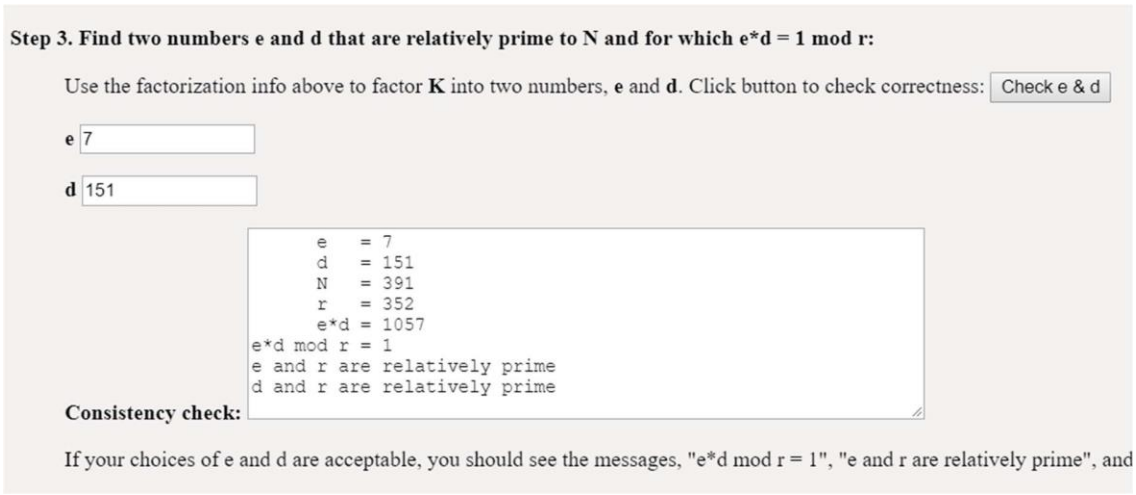
- Step 2:

Select a number where it satisfies 1 mod r == 1 and grab two prime factors (they should not be very large, It will expensive in terms of computation in Encryption and decryption we need to do power of that key in process)



- Step 3:

Check that is it compatible number for the encryption process.



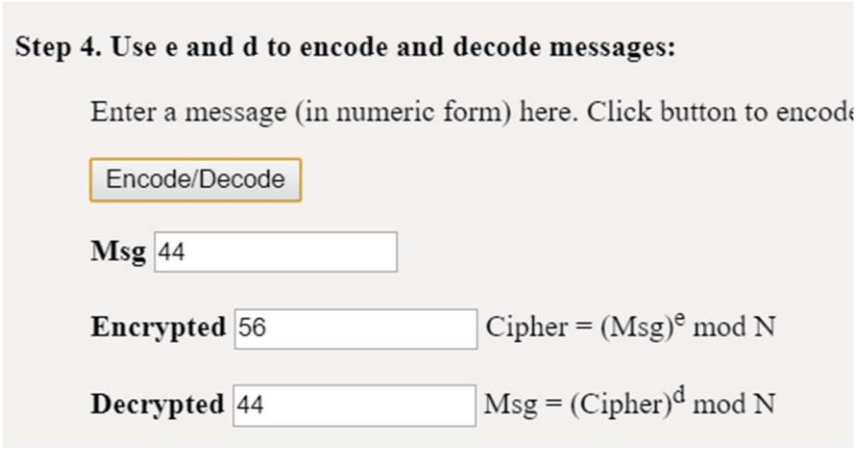
- Step 4:

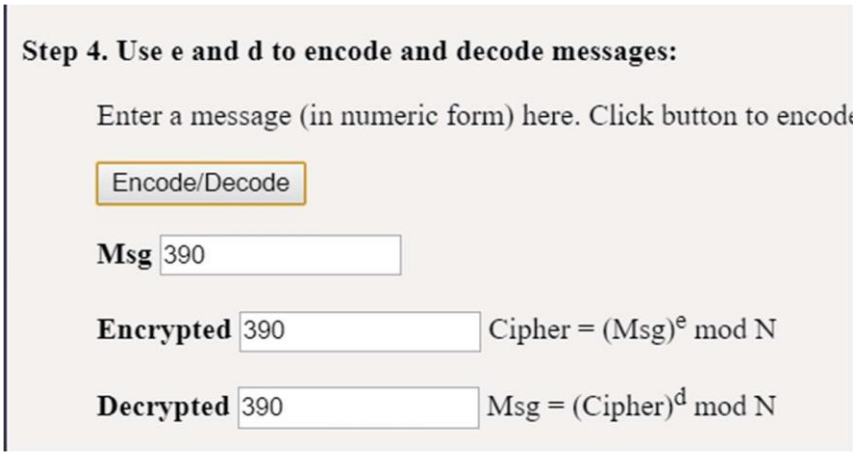
Check that is Encryption is working or not.

Equation : encodedMessage = (Message)^e mod N

decodedMessage = (encodedMessage)^d mod N

where e = public key , d = private key





- **Can we encrypt whole files with RSA encryption ?**

Even though , this algorithm only encode or decode numeric values , we can encrypt files and many other things with data because after all the computer works on numeric values(ANSII Value) BUT , this algorithm is highly computation intensive to perform and the it largely depends on keys value to predict how much time it will take. In Practical scenario , It will be not good choice to use RSA encryption for files/large data. After seeing the methodology we can conclude that we can not use standalone RSA for all the work (Slow and inefficient Encoding and decoding).

So how can we reduce time and processing power without compromising the security. The solution is to use hybrid encryption. The data will be encrypted by traditional method by using some random key and we will encrypt only the random key and then do data transfer and the receiver will decrypt the message by his private key and he will find the tradition key in it and then he will decrypt the whole file with efficiency and speed. Thus , we used both pros of tradition encryption as well as RSA encryption without losing speed or security.

It is better than tradition symmetrical encryption (where we can encoded and decode by same key) because it requires to have special secure line to transfer common key with receiver. (which can be expensive to maintain as well as problematic if some hacker get the access of it)

NOTE : The Receiver will encrypt the data with Sender’s public key and vice versa.